44. (Amended) A method according to claim 34, wherein a Hamming weight indicating the number of "1" bits ["1s"] of an n-bit long bit sequence x is defined as H(x), and an absolute value of a difference between the Hamming weight H(a) of the mask a and a Hamming weight $H(\bar{a})$ of bit inversion $\bar{a}$ of the mask a is less than n/2.

Please add new claim 51 as follows:

--51. An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs (ai, $\bar{a}i$) (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every predetermined period of time;

means for masking bits dependent on a plaintext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from a ciphertext before the ciphertext is output.--

REMARKS

By this Preliminary Amendment, Applicants have amended the specification, amended claims 43 and 44, and added new claim 51.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N.W.
WASHINGTON, D.C. 20005
202-408-4000